The Patent Office
PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
INVESTOR IN PEOPLE

Application No: GB0424653.4 **Examiner:** Mr Adam Tucker

Claims searched: 1-38 **Date of search:** 11 March 2005

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-10, 12-24, 28, 29 & 31-38	US6216014 B1 (Proust et al.) See in particular the abstract, col 1 lines 11-14, col 2 line 62-col 3 line 7, col 3 line 42-col 4 line 28, col 5 lines 9-22, col 9 lines 29-45, col 10 lines 43-52, col 11 lines 22-40 and Appendix 1 col 18
X	1, 3, 4, 6, 20-23, 28, 29 & 31-38	WO00/69183 A2 (Nokia Mobile Phones) See in particular page 1 lines 3-6, page 8 lines 19-24, page 10 line 13-page 13 line 21 and page 15 lines 1-6
X	1-24, 28, 29, & 31-38	EP1357525 A2 (NTT DoCoMo) See in particular the abstract and paras 2, 6, 7, 18, 19, 23, 38, 53-56, 61-74, 76, 77 & 82
X	1-7, 12-24, 28, 29 & 31-38	EP1255179 A2 (Microsoft) See in particular paras 9 & 19-27
X	1, 3-6, 20-24 & 28-38	EP0644513 A2 (AT&T) See in particular the abstract and abstract Figure, col 19 lines 28-42 and claim 1
A,E	-	EP1367843 A1 (Schlumberger Systemes) See in particular the abstract and paras 3, 6, 9 & 10

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC[X] :

G4A; H4L

Worldwide search of patent documents classified in the following areas of the IPC[07]

G06F; H04L; H04M; H04Q

The following online and other databases have been used in the preparation of this search report

WPI, EPODOC

Your ref :	Identities (UK)	**Examiner :**	Mr Adam Tucker
Application No:	GB0424653.4	**Tel :**	01633 814745
Applicant :	Intuwave Limited	**Date of report :**	14 March 2005
Latest date for reply:	7 November 2005	Page 1/5	

Patents Act 1977
Combined Search and Examination Report under Sections 17 & 18(3)

Novelty

1. The invention as defined in claims 1-10, 12, 13, 16, 17, 20-22, 24, 28-33 and 36-38 is not new because it has already been disclosed in each of the following documents:

US 6216014 B1	(Proust et al.)	See in particular the abstract, col 1 lines 11-14, col 2 line 62-col 3 line 7, col 3 line 42-col 4 line 28, col 5 lines 9-22, col 9 lines 29-45, col 10 lines 43-52, col 11 lines 22-40 and Appendix 1 col 18
WO 00/69183 A2	(Nokia Mobile Phones)	See in particular page 1 lines 3-6, page 8 lines 19-24, page 10 line 13-page 13 line 21 and page 15 lines 1-6
EP 1357525 A2	(NTT DoCoMo)	See in particular the abstract and paras 2, 6, 7, 18, 19, 23, 38, 53-56, 61-74, 76, 77 & 82
EP1255179 A2	(Microsoft)	See in particular paras 9 & 19-27
EP 0644513 A2	(AT&T)	See in particular the abstract and abstract Figure, col 19 lines 28-42 and claim 1

2. **US 6216014** anticipates claims 1-10, 12, 13, 16, 24, 28, 29, 31, 32, 33, 37 and 38. This document discloses a mobile telephone in which accessible files are given at least one access control policy which defines access conditions to a particular application, each application (entity) being assigned an access control policy indicator (identifier) which is then used to determine access for the requesting application to the requested file(s) (resource). This appears to anticipate associating an identity (access control policy indicator) with a permission state, wherein the identity (policy indicator) is a label applicable to one of several entities (requesting application programs) on whose behalf the resource (file) could potentially be used as claimed in claims 1, 6, 12, 13, 16, 24, 28, 29, 31, 32, 33, 37 and 38.

[Examination Report contd.]

3. Furthermore, US 6216014 describes that it is the particular application commands, or group of commands, that are assigned access control, see for example Appendix 1. This appears to anticipate claims 2, 7 and 8.

4. Appendix 1 can also be seen to show permission states with a permission type (access condition) and a value (access condition value) as claimed in claim 3. Access conditions or the access control policy indicators are disclosed to be remotely updateable/changeable at column 9 lines 29-45. This anticipates claims 4, 5, 9 and 10.

5. **WO 00/69183** anticipates claims 1, 3, 4, 6, 20, 21, 28, 29, 33, 36, 37 and 38. This document discloses controlling access to applications contained in a SIM card of a mobile telephone by assigning individual application access rights to particular user (entity) profiles (identities) and allowing use of the restricted applications only if the permissions associated with the profile (identity) are acceptable. This anticipates what is claimed in claims 1, 3, 6, 20, 28, 29, 33, 37 and 38. Updating of the profile rights as claimed in claim 4 is also disclosed, for example, at page 15 lines 1-6. It is disclosed at page 12 lines 5-6 that one of the profiles (identities) may be that of the service provider (network operator) as claimed in claim 21. The feature of claim 36 of storing a record of the associated identity and permission state would also seem implicitly anticipated.

6. **EP 1357525** discloses an arrangement for controlling access to data stored on an IC card, for example a mobile telephone SIM card, wherein when access is requested to data on the card both the requesting user's (entity) identity and the application that is requesting the data are checked to determine whether the access is allowed. It is noted that the requesting application itself is associated with an identity which is contained within, and verified from, at least part of a digital signature of the application. If either of the user's identity or the requesting application's identity do not satisfy access requirements to the requested information access is prevented. Furthermore, paragraph 38 also discloses that the result of the access control process is stored in memory, as claimed in claim 36. Therefore this document appears to anticipate each of claims 1, 2, 6, 7, 8, 12, 13, 16, 17, 20, 24, 28, 29, 31, 32 and 36-38.

7. **EP 1255179** discloses access control, in one embodiment on a mobile telephone (para 27) wherein a user, upon 'logging-in' to the mobile phone is assigned a security identification descriptor (SID) which is used to determine whether a particular requesting SID (and therefore the user) is allowed to access a requested resource. Furthermore, the SID is created using a particular authentication method upon log-on and the authentication mechanism may also be checked when a resource is requested, such that there are SID's which have used particular authentication mechanisms are refused. Therefore the access control mechanism not only verifies the requesting user/SID but also verifies the application

[Examination Report contd.]

(script/code) which was used to authenticate the user. This arrangement seems to anticipate claims 1-3, 6, 7, 16, 20, 28, 29, 31, 32, 33 and 38.

8. **EP 0644513** discloses a smartcard, which may be embodied as part of a cellular telephone (column 19 lines 28-42) wherein access to resources on the smartcard/telephone is controlled for particular requesting entities by ID and the ID's associated profile. It is also explicitly disclosed that no particular entity has access to all resources on the smartcard/telephone, as claimed in claim 30. Claims 1, 6, 20, 21, 22, 28-32, 37 and 38 each seem anticipated by what is disclosed in EP 0644513.

Inventive step

9. The invention as defined in claim(s) 3-5, 9-15, 17-24 and 31-37 is obvious in view of what has already been disclosed in the above documents.

10. Following paragraphs 2-4 above, claims 14 and 15 also seem obvious from **US 6216014**. The feature of claim 14 of running the security component outside of the SIM would seem to be an obvious alternative to a person skilled in the art. Use of digital signatures, tokens and confidence levels, e.g. trust levels, are all well known features in security and access control and would seem appropriate to implement in such a system as described in US 6216014 and therefore as claimed in claims 17-19.

11. Furthermore, although the arrangement described in US 6216014 relates to restricting access to files from requesting applications and application commands. It would seem obvious to use the same restricting method and apply it to controlling access from requesting end-users, network operators etc. as claimed in each of claims 20-23.

12. Similarly, although US 6216014 describes controlling access to particular file(s). The same access control method would also seem appropriate to implement in controlling access to hardware, networking or communication resources as claimed in claims 34 and 35.

13. Storage of the associated identity and permission state in the mobile telephone memory would also seem obvious, rendering obvious claim 36.

14. **WO 00/69183** further seems to render obvious claims 22, 23, 31, 32, 34 and 35. This document discloses assigning a profile to potential users and also to the service provider for the mobile telephone. It can be easily envisaged that this arrangement would be extended to also provide a profile for other parties such as the mobile phone

[Examination Report contd.]

manufacturer or application developer/vendor or an employer as claimed in claims 22 and 23.

15. Furthermore, although the method described in WO 00/69183 relates to restricting and controlling access to specific requested resources, to a person skilled in the art, using the same technique would be readily obvious to apply to restricting access to requested data as claimed in claim 31. Access to data including reading, modification or deletion as claimed in claim 32 would therefore also seem to be obvious. Furthermore, controlling access to specific hardware resources or networking/communication resources on the mobile telephone as claimed in claims 34 and 35 would also similarly seem obvious.

16. Following paragraph 6 above **EP 1357525** also seems to render obvious at least claims 3-5, 9-11, 14, 15, 18, 19, 21-23 and 33-35. Each of the features of these claims is considered to relate to features that are well-known in the art and would appear obvious to implement in, or apply to, the access control method as described in EP 1357525.

17. Following paragraph 7 above, **EP 1255179** also appears to render obvious at least claims 4, 5, 12-15, 17-19, 21-24 and 34-37 as these relate to features that are well-known in the art or relate to embodiments that relate to a mobile telephone implementation of the method, which is not described in detail in EP 1255179 but would appear obvious in a mobile telephone embodiment.

18. Following paragraph 8 above **EP 0644513** also seems to render obvious at least claims 3, 4, 5, 23, 24 and 33-36. None of these features of these claims is explicitly disclosed in the disclosure of EP 0644513 but each relates features that would seem readily obvious, such as updating of the access rights stored in a profile or alternatively controlling access to specific applications or hardware/networking/communication resources.

Clarity

19. There are currently two claims numbered 23.

20. Claim 27 is obscure is scope [and was not considered during examination of novelty and inventive step].

Other Matters

21. Please ensure any amendments filed to the claims are reflected with corresponding amendments to the summary of the invention on pages 3-6.

[Examination Report contd.]

22. Please note that due to the number of claims and number of apparent relevant documents, at this stage no detailed consideration has been given to possible combinations of documents/prior art disclosures. However I note that, as acknowledged on page 3 of the description, conceptually similar approaches have been used, and are widely known and applied, in relation to access control for networked computers. Such methods would seemingly be obvious to a person skilled in the art to apply to a mobile telephone which is implicitly networked and may be used, for example, by more than one person or entity, this in itself also being well-known (for example, as can be seen by the above citations).

23. I also note that although the citations above have not been cited against all of the claims, further searching and/or additional searching, which may be necessary after amendments have been filed, may provide examples of embodiments such that these other claims may also be anticipated and/or obvious. As examples, claims 25 and 26, which relate to telephone booting operations and timer operations respectively, which are well-known operations, have not specifically been searched at this stage in the context of access control as they are minor appendant claims. However, if amendment is made to the claims which place more emphasis on these claims, please note that further and/or additional searching may be required.